From: CyberheistNews
To: Rodil, Belinda
Subject: [Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!
Date: Tuesday, March 5, 2019 8:02:57 AM

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Email not displaying?
View Knowbe4 Blog

CyberheistNews Vol 9 #10 | March 5th., 2019

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.

Hal Lonas, Webroot's CTO said: “We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year’s report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program.”

We could not agree more. Here are some highlights:

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:
https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes

[Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:
https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally

[March Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

We listened! KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it’s time for risk assessments and audits.

- [NEW] **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of

maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!
https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60

Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/

Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly ‘security awareness’ trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test.** Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica*.

Try to Spoof Me!
https://info.knowbe4.com/dst-sweepstake-mar2019

*Terms and Conditions apply.

Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

Save My Spot!
https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN

If This Is Your First Issue of CyberheistNews...

CyberheistNews is the world's largest e-zine for IT professionals about social engineering and security awareness training, it is published by KnowBe4 Inc, arrives in your inbox once a week and looks at IT security from the human side. KnowBe4 has partnered with Kevin Mitnick to create new school Security Awareness Training combined with regular simulated phishing attacks.

In CyberheistNews we aim to help you keep your network safe with important news, hints, and tips so that you are aware of the latest social engineering scams and can do something about it.

KnowBe4 lives 100% in the cloud, we use SalesForce as our CRM and via the www.dealsignal.com service we licensed your address. Consider this your sample issue. You can unsubscribe at any time (a few lines below), and you will stop receiving any and all further email.

Are You at RSA This Week? Get Your Free Book Signed by Kevin Mitnick at KnowBe4’s Booth

Get Your Free Book Signed by Kevin Mitnick: Drop by KnowBe4’s Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the ‘World’s Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!
https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever

Warm Regards,
Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

Quotes of the Week

"It isn't where you came from; it's where you're going that counts." - Ella Fitzgerald, Singer (1917 - 1996)

"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."
- Dalai Lama (born 1935)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes

Security News

The Dark Side of the Kremlin: Hacked Russian Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:
https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html

Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker's bank account.

These scams are the highest risk facing the legal sector, according to the UK's Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as 'Friday afternoon Fraud' or 'Monday morning Fraud,' because attackers often strike when they know employees aren't at the top of their game. "Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won't be noticed until a few days later," she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

"The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing," he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today's Conveyancer has the story: https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/

The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim's tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.“

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/

Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as “More_eggs.” More_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy.
Proofpoint has the story:
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."
Thanks,
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."
A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"
- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation: http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-

800m-valuation/

2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware: https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert
3. Deep Learning vs. Machine Learning: A Simple Explanation: https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08
4. New Facebook Phishing Scam is So Good It Will Fool Even You: https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you
5. Comcast set mobile pins to “0000,” helping attackers steal phone numbers: https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/
6. The hacker’s paradise: Social networks net criminals USD 3 billion a year in illicit profits: https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/
7. Enterprises are blind to over half of malware sent to their employees due to SSL: https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/
8. New Attacks Show Signed PDF Documents Cannot Be Trusted: https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted
9. NIST Issues Revised Guidance on Email Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
10. North Korean hackers go on phishing expedition before Trump-Kim summit: https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/

Prepared in cooperation with the CyberWire research team.

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within ‘Stone’s Throw’ of Unicorn Status with Latest KKR Investment: https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/

The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks: https://www.flixxy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4

- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel: https://www.flixxy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret: https://www.flixxy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond: https://www.flixxy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive: https://gizmodo.com/video/3641115?
- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS: https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered: https://www.flixxy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar: https://www.flixxy.com/weird-al-yankovic-word-crimes.htm?utm_source=4
- Imagine having gecko strength. Very cool robot gripper by NASA JPL: https://mobile.twitter.com/CNET/status/1101618114725400576

FOLLOW US ON: Twitter | LinkedIn | YouTube

This email was sent to **brodil@pd.sandiego.gov** by **DoNotReply@knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

1-Click Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com

From: CyberheistNews
To: Cleavinger, John
Subject: [Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!
Date: Tuesday, March 5, 2019 8:08:36 AM

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Email not displaying?
View Knowbe4 Blog

CyberheistNews Vol 9 #10 | March 5th., 2019

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.

Hal Lonas, Webroot's CTO said: “We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year’s report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program.”

We could not agree more. Here are some highlights:

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:
https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes

[Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:
https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally

[March Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

We listened! KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it’s time for risk assessments and audits.

- [NEW] **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of

maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!
https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60

Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/

Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly ‘security awareness’ trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test.** Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica*.

Try to Spoof Me!
https://info.knowbe4.com/dst-sweepstake-mar2019

*Terms and Conditions apply.

Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

Save My Spot!
https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN

If This Is Your First Issue of CyberheistNews...

CyberheistNews is the world's largest e-zine for IT professionals about social engineering and security awareness training, it is published by KnowBe4 Inc, arrives in your inbox once a week and looks at IT security from the human side. KnowBe4 has partnered with Kevin Mitnick to create new school Security Awareness Training combined with regular simulated phishing attacks.

In CyberheistNews we aim to help you keep your network safe with important news, hints, and tips so that you are aware of the latest social engineering scams and can do something about it.

KnowBe4 lives 100% in the cloud, we use SalesForce as our CRM and via the www.dealsignal.com service we licensed your address. Consider this your sample issue. You can unsubscribe at any time (a few lines below), and you will stop receiving any and all further email.

Are You at RSA This Week? Get Your Free Book Signed by Kevin Mitnick at KnowBe4's Booth

Get Your Free Book Signed by Kevin Mitnick: Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!
https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever

Warm Regards,
Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

Quotes of the Week

"It isn't where you came from; it's where you're going that counts." - Ella Fitzgerald, Singer (1917 - 1996)

"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."
- Dalai Lama (born 1935)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes

Security News

The Dark Side of the Kremlin: Hacked Russian Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:
https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html

Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker's bank account.

These scams are the highest risk facing the legal sector, according to the UK's Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as 'Friday afternoon Fraud' or 'Monday morning Fraud,' because attackers often strike when they know employees aren't at the top of their game. "Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won't be noticed until a few days later," she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

"The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing," he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today's Conveyancer has the story: https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/

The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim's tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won't threaten to involve law enforcement without warning. As a general rule of thumb, if you don't already know that you have past-due tax bills or other missed payments, the first time you find out about them won't be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don't click on any links and instead go directly to the IRS' website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should "approach all emails with caution, even those from people you know."

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/

Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More_eggs." More_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It’s previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don’t attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don’t know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they’re absolutely certain of their legitimacy.
Proofpoint has the story:
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."
Thanks,
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP’s that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We’ve sold this once to an Aerospace company last year and we’re slow to get things going as we’re a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."
A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"
- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation: http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-

800m-valuation/

2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware: https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert
3. Deep Learning vs. Machine Learning: A Simple Explanation: https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08
4. New Facebook Phishing Scam is So Good It Will Fool Even You: https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers: https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits: https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/
7. Enterprises are blind to over half of malware sent to their employees due to SSL: https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/
8. New Attacks Show Signed PDF Documents Cannot Be Trusted: https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted
9. NIST Issues Revised Guidance on Email Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
10. North Korean hackers go on phishing expedition before Trump-Kim summit: https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/

Prepared in cooperation with the CyberWire research team.

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment: https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/

The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks: https://www.flixxy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4

- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel: https://www.flixxy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret: https://www.flixxy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond: https://www.flixxy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive: https://gizmodo.com/video/3641115?
- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS: https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered: https://www.flixxy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar: https://www.flixxy.com/weird-al-yankovic-word-crimes.htm?utm_source=4
- Imagine having gecko strength. Very cool robot gripper by NASA JPL: https://mobile.twitter.com/CNET/status/1101618114725400576

FOLLOW US ON: Twitter | LinkedIn | YouTube

This email was sent to **jrcleavinger@pd.sandiego.gov** by **DoNotReply@knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

1-Click Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com

From: CyberheistNews
To: Smith, George
Subject: [Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!
Date: Tuesday, March 5, 2019 7:49:56 AM

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Email not displaying?
View Knowbe4 Blog

CyberheistNews Vol 9 #10 | March 5th., 2019

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.

Hal Lonas, Webroot's CTO said: “We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year’s report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program.”

We could not agree more. Here are some highlights:

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.
- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:
https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes

[Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:
https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally

[March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

We listened! KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it’s time for risk assessments and audits.

- [NEW] **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of

maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!
https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60

Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/

Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly ‘security awareness’ trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test.** Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica*.

Try to Spoof Me!
https://info.knowbe4.com/dst-sweepstake-mar2019

*Terms and Conditions apply.

Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

Save My Spot!
https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN

Are You at RSA This Week? Get Your Free Book Signed

by Kevin Mitnick at KnowBe4's Booth

Get Your Free Book Signed by Kevin Mitnick: Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!
https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever

Warm Regards,
Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

Quotes of the Week

"It isn't where you came from; it's where you're going that counts." - Ella Fitzgerald, Singer (1917 - 1996)

"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."
- Dalai Lama (born 1935)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes

Security News

The Dark Side of the Kremlin: Hacked Russian

Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a "transparency collective" made up of mostly Ukrainian and Russian "hacktivists".

The massive data leak, dubbed "The Dark Side of the Kremlin," includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin's inner circle. Some of the documents seem to provide insights into Russia's activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:
https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html

Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today's Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker's bank account.

These scams are the highest risk facing the legal sector, according to the UK's Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as 'Friday afternoon Fraud' or 'Monday morning Fraud,' because attackers often strike when they know employees aren't at the top of their game. "Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won't be noticed until a few days later," she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

"The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing," he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today's Conveyancer has the story: https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/

The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim's tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won't threaten to involve law enforcement without warning. As a general rule of thumb, if you don't already know that you have past-due tax bills or other missed payments, the first time you find out about them won't be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don't click on any links and instead go directly to the IRS' website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should "approach all emails with caution, even those from people you know."

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/

Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More_eggs." More_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy.

Proofpoint has the story:
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."
Thanks,
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."
A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"
- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation: http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware: https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert
3. Deep Learning vs. Machine Learning: A Simple Explanation: https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08
4. New Facebook Phishing Scam is So Good It Will Fool Even You: https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you
5. Comcast set mobile pins to “0000,” helping attackers steal phone numbers: https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits: https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:
https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/

8. New Attacks Show Signed PDF Documents Cannot Be Trusted: https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted
9. NIST Issues Revised Guidance on Email Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
10. North Korean hackers go on phishing expedition before Trump-Kim summit: https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/

Prepared in cooperation with the CyberWire research team.

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within ‘Stone’s Throw’ of Unicorn Status with Latest KKR Investment: https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks: https://www.flixxy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel: https://www.flixxy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret: https://www.flixxy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond: https://www.flixxy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

https://gizmodo.com/video/3641115?

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS: https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered: https://www.flixxy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar: https://www.flixxy.com/weird-al-yankovic-word-crimes.htm?utm_source=4
- Imagine having gecko strength. Very cool robot gripper by NASA JPL: https://mobile.twitter.com/CNET/status/1101618114725400576

FOLLOW US ON: Twitter | LinkedIn | YouTube

From: CyberheistNews
To: Fornes, Michael
Subject: [Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!
Date: Tuesday, March 5, 2019 7:49:57 AM

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Email not displaying?
View Knowbe4 Blog

CyberheistNews Vol 9 #10 | March 5th., 2019

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.

Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

We could not agree more. Here are some highlights:

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.
- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:
https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes

[Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:
https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally

[March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

We listened! KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it’s time for risk assessments and audits.

- [NEW] **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of

maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!
https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60

Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/

Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly ‘security awareness’ trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test.** Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica*.

Try to Spoof Me!
https://info.knowbe4.com/dst-sweepstake-mar2019

*Terms and Conditions apply.

Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

Save My Spot!
https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN

Are You at RSA This Week? Get Your Free Book Signed

by Kevin Mitnick at KnowBe4’s Booth

Get Your Free Book Signed by Kevin Mitnick: Drop by KnowBe4’s Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the ‘World’s Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!
https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever

Warm Regards,
Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

Quotes of the Week

"It isn't where you came from; it's where you're going that counts." - Ella Fitzgerald, Singer (1917 - 1996)

"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."
- Dalai Lama (born 1935)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes

Security News

The Dark Side of the Kremlin: Hacked Russian

Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:
https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html

Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/

The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.“

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/

Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as “More_eggs.” More_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It’s previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don’t attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don’t know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they’re absolutely certain of their legitimacy.

Proofpoint has the story:
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."
Thanks,
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."
A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"
- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation: http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware: https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert
3. Deep Learning vs. Machine Learning: A Simple Explanation: https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08
4. New Facebook Phishing Scam is So Good It Will Fool Even You: https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you
5. Comcast set mobile pins to “0000,” helping attackers steal phone numbers: https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits: https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:
https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/

8. New Attacks Show Signed PDF Documents Cannot Be Trusted: https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted
9. NIST Issues Revised Guidance on Email Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
10. North Korean hackers go on phishing expedition before Trump-Kim summit: https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/

Prepared in cooperation with the CyberWire research team.

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment: https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks: https://www.flixxy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel: https://www.flixxy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret: https://www.flixxy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond: https://www.flixxy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

https://gizmodo.com/video/3641115?

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS: https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered: https://www.flixxy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar: https://www.flixxy.com/weird-al-yankovic-word-crimes.htm?utm_source=4
- Imagine having gecko strength. Very cool robot gripper by NASA JPL: https://mobile.twitter.com/CNET/status/1101618114725400576

FOLLOW US ON: Twitter | LinkedIn | YouTube

This email was sent to **mfornes@pd.sandiego.gov** by **DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

1-Click Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com

From: CyberheistNews
To: Daly, Brendan
Subject: [Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!
Date: Tuesday, March 5, 2019 7:48:05 AM

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Email not displaying?
View Knowbe4 Blog

CyberheistNews Vol 9 #10 | March 5th., 2019

[Heads-Up] 40 Percent of Malicious URLs Found on *Good* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.

Hal Lonas, Webroot's CTO said: “We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year’s report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program.”

We could not agree more. Here are some highlights:

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:
https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes

[Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:
https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally

[March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

We listened! KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it’s time for risk assessments and audits.

- [NEW] **Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of

maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!
https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60

Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/

Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly ‘security awareness’ trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test.** Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica*.

Try to Spoof Me!
https://info.knowbe4.com/dst-sweepstake-mar2019

*Terms and Conditions apply.

Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

Save My Spot!
https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN

Are You at RSA This Week? Get Your Free Book Signed

by Kevin Mitnick at KnowBe4's Booth

Get Your Free Book Signed by Kevin Mitnick: Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!
https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever

Warm Regards,
Stu Sjouwerman
Founder and CEO
KnowBe4, Inc

Quotes of the Week

"It isn't where you came from; it's where you're going that counts." - Ella Fitzgerald, Singer (1917 - 1996)

"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."
- Dalai Lama (born 1935)

Thanks for reading CyberheistNews
But if you want to unsubscribe, you can do that right here

You can read CyberheistNews online at our Blog
https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes

Security News

The Dark Side of the Kremlin: Hacked Russian

Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a "transparency collective" made up of mostly Ukrainian and Russian "hacktivists".

The massive data leak, dubbed "The Dark Side of the Kremlin," includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin's inner circle. Some of the documents seem to provide insights into Russia's activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:
https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html

Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today's Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker's bank account.

These scams are the highest risk facing the legal sector, according to the UK's Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as 'Friday afternoon Fraud' or 'Monday morning Fraud,' because attackers often strike when they know employees aren't at the top of their game. "Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won't be noticed until a few days later," she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/

The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.“

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/

Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as “More_eggs.” More_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It’s previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don’t attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don’t know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they’re absolutely certain of their legitimacy.

Proofpoint has the story:
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."
Thanks,
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."
A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"
- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation: http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware: https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert
3. Deep Learning vs. Machine Learning: A Simple Explanation: https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08
4. New Facebook Phishing Scam is So Good It Will Fool Even You: https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers: https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits: https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/
7. Enterprises are blind to over half of malware sent to their employees due to

SSL: https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/

8. New Attacks Show Signed PDF Documents Cannot Be Trusted: https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted
9. NIST Issues Revised Guidance on Email Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
10. North Korean hackers go on phishing expedition before Trump-Kim summit: https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/

Prepared in cooperation with the CyberWire research team.

Cyberheist 'Fave' Links

This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment: https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks: https://www.flixxy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel: https://www.flixxy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret: https://www.flixxy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond: https://www.flixxy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

https://gizmodo.com/video/3641115?

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS: https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered: https://www.flixxy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar: https://www.flixxy.com/weird-al-yankovic-word-crimes.htm?utm_source=4
- Imagine having gecko strength. Very cool robot gripper by NASA JPL: https://mobile.twitter.com/CNET/status/1101618114725400576

From: Daly, Brendan
To: Jordon, Jeffrey
Subject: RE: FYI
Attachments: image001.jpg

Yes, I did see this in one.
Thanks

Brendan M. Daly, MS
Cyber Security Program Coordinator
City of San Diego
Police Department

[redacted]

CONFIDENTIAL COMMUNICATIONS
This electronic mail message and any attachments are intended only for the use of the addressee(s) named above and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not an intended recipient, or the employee or agent responsible for delivering this e-email to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you received this e-mail message in error, please immediately notify the sender by replying to this message or by telephone. Thank you.

From: Jordon, Jeffrey [redacted]
Sent: Monday, June 22, 2020 2:34 PM
To: Daly, Brendan [redacted]
Subject: FYI

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Don't know if you are familiar with the above issue –

Jeff Jordon, Captain
San Diego Police Department
Special Projects/Legislative Affairs
[redacted]